Specification:

Field of Invention: Insert as paragraph 2-

A2

More specifically and simply put, the invention is a designed to detect (and reverse damages caused by) a social and criminal phenomenon, commonly known as "identity theft".

Description of Prior Art: Insert as paragraph 3 and 4-

A3

Automated handlings of personal information for purpose not related to crime prevention have been the subject of earlier patents. O'Flaherty teaches of systems and methods of data warehousing and analysis, and in particular to a system and method for enforcing privacy constraints on a database management system. Freishtat discloses an internet related method for aggregation of personal information for direct marketing and purposes of marketing and end user convenience.

None of the prior art discussed possesses the novelty of prevention, detection, and reversal of criminal or unauthorized personal identity data point appropriation

Summary: Insert as paragraph 2-

A4

More specifically, the invention is a designed to detect patterns that are the indicia of computer and internet crimes related to the theft of personal data, and to reverse damages caused by said crimes.

NE

Specific Embodiment of the Invention: Insert as Specific Embodiment of the Invention –

One embodiment of the invention is based upon a Microsoft Windows 2000 Server (formerly Windows NT) platform. This embodiment uses the programming language VBScript which is held inside Active Server Pages. Further, Microsoft SQL Server 2000 is used as a data warehouse. The data warehouse contains end user information, replicated databases from a plurality of sources including credit reporting services, government records (including court records, records of deeds and liens, criminal databases), which is continuously updated, and tables where records containing the indicia of Identity theft have been inserted and are continuously updated as new methods of Identity theft develop. Said data warehouse uses merge-based replication over a secure internet channel of all source databases.

This embodiment resides on a Compaq Proliant Server 6500 with 1 gigabyte of random access memory, and 200 gigabytes of data storage, which is structured in a redundant array of independent disks (RAID, level 5). This array is mirrored so that in the event of failure, the system will automatically switch to use of the mirrored databases. The disks are hot-pluggable—that is, they can be removed from the system without turning off the server, and a new disk can be inserted, and then populated with data, all without interruption of the invention. Active Server Pages are used for dynamic generation of internet web pages specific to the end user. A 128-byte secured socket layers is utilized to ensure that private data transmitted to or from the memory controller (1) is not readable in transmission.

The program code performs all logical operations. The most important operations include the collection of user data, the replication of an unlimited number of databases (7). Microsoft SQL Server 2000 is able to replicate a plurality of databases (7) that are not made or manufactured by Microsoft, and this feature is utilized to replicate the plurality of databases (7) which use databases such as DB2, Oracle, Sybase and others.

Further logical operations allow for the input of data regarding the indicia of Identity theft. As said Identity theft is a constantly evolving problem, new methods for Identity theft are constantly being utilized. As a new indicia is made known, or otherwise discovered, a pattern indicating that indicia is input. The entirety of this database is used to analyze end user data as against the plurality of data sources (7) and a logical operation trips, and notice is given via the Internet when such indicia occurs or is present.

The communication port is a high-speed (T-1) connection to the Internet. This port consists of a CSU/DSU to connect to a specific provider of high-speed Internet service. A Cisco firewall is used to protect the invention from unauthorized use or monitoring, and to notify a system operator when said use or monitoring occurs.

Active Server Pages allow for graphically representation of the presence and risk of the indicia of Identity theft. In this embodiment, the graphical representation is akin to that of a traffic light. A graphic of a green light signifies public information that is present but according to the present invention, not the indicia of Identity theft. A yellow light indicates that the information found relative to the end user could be used for the purposes of identity theft. A graphic of a red light indicates that the indicia of Identity theft is present.

Next to these representations are buttons which afford the end user the opportunity, on a plurality of end user devices, to take action with regard to any information. These actions include removal, notification of error to the data source provider, removal or request for removal from the data source provider and referral to law enforcement. The types of actions are also dynamic and specific to new and dynamic indicia of Identity theft and new form of Identity theft.

A regular and automatic backup routine using a tape drive (manufactured by Syquest with associated software and scripts) are made to ensure the integrity of a very large and highly dynamic set of data sources.